data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected, and wherein the processing unit is adapted to determine the tag value to be the selected symbol.

REMARKS/ARGUMENTS

1. Claim Rejections - 35 USC § 112

Examiner has rejected claims 10 and 11 under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. Claims 10 and 11 have been amended to overcome the rejection. Support for amended claims 10 and 11 can be found at least at page 5, lines 20-27.

2. Claim Rejections – 35 U.S.C. § 101

Claims 10 and 11 stand rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Although claims 10 and 11 have been amended to better define the invention, Applicant again traverses the rejection. To the extent the Examiner persists in maintaining the rejection, Applicant would request the Examiner and the Supervisory Examiner Kim Vu call the Applicant's attorney of record to discuss the matter. Previous attempts to contact the Examiner to discuss the matter have not been successful. The Examiner rejected claims 10-11 under 35 U.S.C. §101. According to the Examiner on Page 5 of the Office Action:

> Claim 10 and 11 recite "a computer program product configured to process a message to determine a tag value from the message and from a key according to a message authentication code." The claim is clearly a software program and it is non-statutory as not being tangibly embodied in a manner so as to be executable. Software program/product is unpatentable.
> Furthermore, applicant has pointed out in the specification (see lines 6-14 of page 5) **"the following may be implemented in software and carried out in a data processing system or other processing means caused by the execution of computer-executable instructions. The**

instructions may be program code means loaded in a memory, such as a RAM, from a storage medium or from another computer *via* a *computer network*. Alternatively, the described features may be implemented by hardwired circuitry instead of software or in combination with software", which clearly including intangible media such as signals, carrier waves, transmissions, optical waves, transmission media or other media incapable of being touched or perceived absent the tangible medium through which they are conveyed. Therefore, claims 10 and 11 recite a non-statutory subject matter. In addition, applicant's computer program product are not tied to a particular machine and do not perform a transformation. Thus, the claims are non-statutory.

Applicant respectfully traverses the rejection. The Examiner states that *the Specification* does not meet the 35 U.S.C. §101 condition. From that premise, the Examiner concludes that claims 10 and 11 are non-statutory. However, it is well known that *the claims* define the scope of the claimed invention. Paragraph 7.05.01 of the MPEP provides guidance for rejecting claims based on 35 U.S.C. §101 (emphasis added):

> ...the *claimed invention* is directed to non-statutory subject matter because [1]
> Examiner Note
> In bracket 1, explain why the *claimed invention* is not patent eligible subject matter, e.g.,
> (a) why the *claimed invention* does not fall within at least one of the four categories of patent eligible subject matter recited in 35 U.S.C. 101 (process, machine, manufacture, or composition of matter); or
> (b) why the *claimed invention* is directed to a judicial exception to 35 U.S.C. 101 (i.e., an abstract idea, natural phenomenon, or law of nature) and is not directed to a practical application of such judicial exception (e.g., because the *claim* does not require any physical transformation and the invention as claimed does not produce a useful, concrete, and tangible result); or
> (c) why the *claimed invention* would impermissibly cover every substantial practical application of, and thereby preempt all use of, an abstract idea, natural phenomenon, or law of nature.

Nowhere in claims 10 or 11 does the Applicant claim as part of his invention the elements ascribed thereto by the Examiner (signals, carrier waves, transmissions, optical waves, transmission media or other media incapable of being touched or perceived). Further, the mere fact that the Specification mentions a signal DOES NOT mean the invention as claimed is non-statutory.

The Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility ("Guidelines"), Section 2106 of the MPEP provides, in pertinent part, as follows (emphasis added):

II. DETERMINE WHAT APPLICANT HAS INVENTED AND IS SEEKING TO PATENT

It is essential that patent applicants obtain a prompt yet complete examination of their applications. Under the principles of compact prosecution, **_each claim_ should be reviewed for compliance with every statutory requirement for patentability** in the initial review of the application, even if one or more claims are found to be deficient with respect to some statutory requirement. Thus, USPTO personnel should state all reasons and bases for rejecting claims in the first Office action. Deficiencies should be explained clearly, particularly when they serve as a basis for a rejection. Whenever practicable, USPTO personnel should indicate how rejections may be overcome and how problems may be resolved. A failure to follow this approach can lead to unnecessary delays in the prosecution of the application.

C. Review the Claims

The claims define the property rights provided by a patent, and thus require careful scrutiny. **The goal of claim analysis is to identify the boundaries of the protection** sought by the applicant and to understand how the claims relate to and define what the applicant has indicated is the invention. USPTO personnel must first determine the scope of a claim by thoroughly analyzing the language of the claim before determining if the claim complies with each statutory requirement for patentability. See In re Hiniker Co., 150 F.3d 1362, 1369, 47 USPQ2d 1523, 1529 (Fed. Cir. 1998) ("[T]he name of the game is the claim.").

USPTO personnel should begin claim analysis by identifying and evaluating each claim limitation. For processes, the claim limitations will define steps or acts to be performed. For products, the claim limitations will define discrete physical structures or materials. Product claims are claims that are directed to either machines, manufactures or compositions of matter.

USPTO personnel are to correlate each claim limitation to all portions of the disclosure that describe the claim limitation. This is to be done in all cases, regardless of whether the claimed invention is defined using means or step plus function language. The correlation step will ensure that USPTO personnel correctly interpret each claim limitation.

As noted, the Examiner states that *the Specification* does not meet the 35 U.S.C. §101 condition. Notably, the Applicant does not even refer to these supposedly claimed non-statutory claim elements. Rather, the Examiner first *implies* non-statutory claim elements into the Specification, and then reads these claim elements into claims 10 and 11, so as to reject the present application.

Applicant is unaware of a requirement that a Specification be silent as material that is non-statutory subject matter, lest it be incorporated into the claims. In fact, many issued patents *expressly* describe within the Specification, *but do not claim*, signals, mathematical algorithms, laws of nature, etc., in order to provide the public with a fuller understanding of the claimed invention. Applicant does not believe that a patent whose Specification refers to, or can be implied to refer to, e.g., how an apparatus processes a signal, is subject to invalidation because the claims thereof must be interpreted as incorporating the non-statutory claim element of the signal itself (as part of the apparatus). If such were the case, any patent on a wireless or computer related apparatus, all of which process signals, would be invalid, even though the signal itself is not expressly claimed.

Applicant respectfully submits that the Examiner has incorrectly asserted that a Specification (as opposed to the claims) must meet the requirements of 35 U.S.C. §101, and further, has impermissibly fashioned additional material as being implied in the Specification, and then has impermissibly deemed such fashioned material as being incorporated from the Specification as claim elements of claims 10 and 11. Hence, favorable reconsideration of claims 10 and 11 is respectfully requested in view of the amendments and foregoing remarks.

3. Claim Rejections – 35 U.S.C. § 103(a)

Claims 1-5, 7-12 remain rejected under 35 U.S.C.103(a) as being unpatentable over Graveman (US 6,851,052 81), and further in view of Carman et al (US 6,845,449 81). The Applicant respectfully traverses the rejection as it is technically impossible to combine these two references to obtain the present invention. Because of this technical inability (as described below) to combine the two, it would not have been obvious to a

person having ordinary skill in the art at the time the invention was made to modify Graveman with the teaching of Carman to authenticate the source and integrity of transmitted or stored information.

The Examiner states in the Office Action:

> ...Graveman teaches an approximate message authentication code (AMAC) which, like conventional message authentication codes, provides absolute authentication of the origin of the message, yet provides an approximate integrity check for the content of the message. The approximate integrity check will be computed probabilistically and will likely be the same for messages having only a small percentage of different bits. A distance measure on the AMACs, such as a Hamming distance measure, may be used to determine whether the number of bit differences between the messages is likely to be within an acceptable amount. The AMAC is a probabilistic checksum based on a shared key. The AMAC uses the message and a shared key as inputs (see abstract of Graveman, and more details of claim 1's limitation are taught by Graveman in column 5, lines 13-40; column 6, line 64 through column 7, line 19; column 8, lines 31-35 of Graveman).

According to the Examiner, the ordinary skilled person would have been motivated to modify Graveman with the teaching of Carman to provide absolute authentication of the source or origin of a received message so as to permit verifying approximate integrity between the original message and the received message.

Applicant strongly insists that Graveman does not "*provide absolute authentication of the source or origin*". There is always, albeit small, a probability that the origin can be successfully spoofed. The fact that there is a distance does not mean that the construction can be used as an error-correcting code. The decoding problem is nondeterministic polynomial (NP) complete, which amongst others, has the consequence that only special constructions that give distance can be decodable. This is not addressed or contemplated or by Graveman.

With respect to Carman, the Examiner states:

> Although Graveman teaches the technique to process message authentication code using initial vectors (which is the symbols of the codeword), Graveman is silent on the capability of showing the details of forming a codeword (e.g., message authentication code or data word) and

the tag value to be the selected symbol. On the other hand, Carman teaches codeword in column 2, lines 1-11; column 20, lines 57-67 of Carman, and tag value in Figures 1, 17A178 and more details in column 3, lines 35-43; column 26, lines 25-36 of Carman. Thus, the combination of teaching between Graveman and Carman teaches the claimed subject matter.

Applicant previously responded, and again responds that Carman is only tangentially related to the present invention as it discuss error-correcting codes. Error-correcting codes and different aspects and encoding methods have been very extensively studied in academic research and industry. Specifically, Carman teaches a method to detect and correct errors by using an authentication mechanism that uses a reversible inner function. Besides the message and the authentication tag, the encrypted inner result is also sent as seen in Figure 15 and Figure 17A. This implies that the length of the data sent is substantially longer than only the message itself and the tag as the length of the encrypted inner result must be about the same as the message itself (for otherwise function 1502 would not be reversible)."

Now when combining Carman and Graveman, there is essentially one option: take Carman and use Graveman instead of SHA-1 in 1506 (Figure 15). The alternative to use Carman in Graveman would be illogical and unworkable. Carman could be placed in front of Graveman but then the input to Graveman would be that tag, the message and the intermediate result. This would destroy the property of Graveman of being an AMAC as one bit change in the message will cause about half of the bits of the intermediate result to change and hence 1/4 of the input bits to Graveman will change which would then ruin the AMAC aspect of Graveman. If one takes Carman and uses Graveman instead of SHA-1 in 1506 (Fig 15), the AMAC property of Graveman is destroyed as, as noted above, half the bits of the intermediate result will flip when changing one bit of the message. Hence one skilled in the art would <u>never</u> combine the two as to do so would add complexity without gaining anything and without obtaining the benefits of either. Furthermore, the Carman construction, which relies heavily on the basic construct in Figure 15, is inefficient as a MAC code which is the sole purpose of the present invention. In Carman, the objective is to detect and correct errors and in doing so, many more bits must be sent than that only needed for MAC functions.

Hence, one skilled in the art would never consider Carman as a MAC function itself. Further, as explained above, using Carman in Graveman destroys Graveman and therefore, one skilled in the art would never combine them. The Examiner has yet to address Applicant's argument with respect to the combination of Carman and Graveman.

Combining the invention of Carman with that of Graveman, or *vice versa*, would substantially change the operation of both and would not result in the present invention. If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious (See *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)). *In re Ratti*, the court reversed the rejection of a patent application holding the "...suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference] as well as a change in the basic principle under which the [primary reference] construction was designed to operate." 270 F.2d at 813, 123 USPQ at 352.

KSR International Co. v. Teleflex Inc. (KSR) requires that an Examiner provide "some articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness." (KSR Opinion at p. 14). An Examiner must "identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does," (KSR Opinion at p. 15). And, the Examiner must make "'explicit" this rationale of "the apparent reason to combine the known elements in the fashion claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "'the background knowledge possessed by a person having ordinary skill in the art." (KSR Opinion at p. 14). Anything less than such an explicit analysis is not be sufficient to support a prima facie case of obviousness. Based upon KSR, the Examiner has failed to show any sufficient reason for combining the references, and therefore the claims are not obvious in view of any combination of the cited references."

The Examiner further rejected claims 5-6 under 35 U.S.C. § 103(a) as being unpatentable over Graveman and further in view of Carman *et al* and Shokrollahi (US 6,631,172). The Applicant respectfully traverse the rejection because, as noted above,

it is technically impossible to combine Graveman and Carman to obtain the present invention. Because of this technical inability to combine the two, it would not have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Graveman with the teaching of Carman and Shokrollahi to authenticate the source and integrity of transmitted or stored information using a Reed-Solomon error correcting code wherein the tag value is determined by evaluating a Reed-Solomon encoding polynomial at a point determined by the key and the tag value is an element in a finite field.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

Date:_____April 23, 2009_____

Michael Cameron
Registration No. 50,298

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024
(972) 583-4145
michael.cameron@ericsson.com